REMARKS/ARGUMENTS

The Applicant acknowledges, with thanks, receipt of the Office Action mailed May 14, 2007. Claims 1-16, 18-19, and 22 are pending. Claims 1-16, 18-19, and 22 stand rejected. Claims 17, 20-21, and 23-27 (renumbered) have been canceled. Accordingly, claims 1, 13, and 19 has been amended to overcome the Examiner's rejection and thus claims 1-16, 18-19, and 22 should now be in condition for allowance. The current Office Action by the Examiner of this application, together with the cited references, has been given careful consideration. Following such consideration, it is respectfully requested that the above-indicated patent application be reconsidered, as amended. No new matter is being added.

1. Renumbered claims 23-27 are objected to for the numbering of these claims being not in accordance with 37 CFR 1.126. Renumbered claims 23-27 are now cancelled.

2. Claims 17 and 19-22 are rejected under 35 U.S.C., second paragraph, as being indefinite. Accordingly, claims 17 and 20-21 are cancelled. Claim 19 is amended to overcome Examiner's rejection.

3. Renumbered claims 23-27 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Accordingly, claims 23-27 are cancelled.

4. Claims 1-27 are rejected under 35 U.S.C. 102 (e) as being anticipated by Cisco Systems, "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", 2002 (Cisco).

The term "***management frame,***" generally refers to data that is transmitted between the station and access point that control the association of the station with the access point. Some examples of management frames include association frames, re-association frames, disassociation frames, deauthentication frames, and so forth, that enable and control respective associations between the station and access point. Management frames are well known to those of ordinary skill in the art. As noted in paragraphs 2 and 4 of the original specification,

traditional security and control efforts have been directed towards protecting the data content of a transmission and towards the protection of management frame packets.

Applicant respectfully submits that independent claim 1 as now amended, recites a method for securing **management frames** comprising establishing an authenticated relationship between a transmitter and a receiver on a network, generating *a client-specific management frame protection key,* deriving an information element *based upon the client-specific management frame protection key* for signing a management frame packet transmitted on the network, embedding the information element into the management frame packet, transmitting the management frame packet to the receiver, receiving the management frame packet and validating the information element in the received management frame packet. The amendments to claim 1 are supported by the original application (see, for example, paragraphs [0042] and [0043]).

Applicant respectfully submits that independent claim 13, as now amended, recites a system for securing a **management frame** packet comprising means for authenticating a relationship between a transmitter and a receiver, means for generating *a client-specific management frame protection key,* means for deriving an information element *based upon the client-specific management frame protection key* for signing the management frame packet transmitted between the transmitter and the receiver via a network, means for adding the information element into the management frame packet, means for transmitting the management frame packet to the receiver via the network, means for receiving the management frame packet, and means for validating the information element in the received management frame packet. The amendments to claim 13 are supported by the original application (see, for example, paragraphs [0042] and [0043]).

Applicant respectfully submits that independent claim 19, as now amended, recites a method for preventing IEEE 802.11 session disruption on a network comprising establishing a communication link between an access point and a wireless client on the network, creating a trust relationship between the access point and the wireless client such that the wireless client is adapted to securely access the network, establishing a client-specific key for signing **a management frame** packet configured to be transmitted between the access point and the wireless client, generating a message integrity check value based upon the client-specific key, calculating a replay protection value for signing the management frame packet, embedding the

message integrity check value and the replay protection value into the **management frame** packet, transmitting the *management frame packet comprising the message integrity check value and the replay protection value* to the access point, and authenticating the *message integrity check value and the replay protection value*. The amendments to claim 13 are supported by the original application (see, for example, paragraph [0044]).

By contrast, Cisco discloses a method and system for securing **data frames**, in which a static or dynamic WEP key is generated and used for security purposes. According to Cisco, a message integrity check (MIC) function and pre-packet keying is provided on WEP-encrypted **data frames** (see, for example, p. 19, section 4.1.3). In addition, Applicant respectfully submits that in p. 12, section 3.2 Statistical Key Derivation, Cisco discusses vulnerability of WEP keys and WEP key derivation in an active network attack. Unlike Cisco, the subject application comprises deriving an information element based upon the client-specific management frame protection key for security purposes. Therefore claims 1 and 13, as currently amended, are not anticipated by Cisco and withdrawal of these rejections is respectfully requested.

Cisco further discloses a method for securing 802.11 Wireless LANs in which a WEP key is generated along with dynamic key rotation for broadcast and multicast traffic. According to Cisco, to augment WEP encryption, pre-packet keying and MIC function are implemented, providing every **data frame** with a new and unique WEP key and MIC feature. Applicant respectfully submits that although Cisco in p. 16, section 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite, does not specifically state that the keying is provided for data frames, however, further in section 4.13. Data Privacy with TKIP, when disclosing details to the Security Suite, Cisco specifically points out that the MIC function and pre-packet keying are provided on WEP encrypted **data frames**. Further, in Figure 26 Cisco illustrates transmitting of an MIC enabled WEP frame format, which is a data format. Therefore claim 19, as currently amended, is not anticipated by Cisco and withdrawal of these rejections is respectfully requested.

Claims 2-12 depend directly or indirectly from claim 1 and therefore contain each and every element of claim 1. Thus, for the reasons already set forth for currently amended claim 1, claims 2-12 are not anticipated by Cisco. Claims 14-16 and 18 depend directly or indirectly from claim 13 and therefore contain each and every element of claim 13. Thus, for the reasons already set forth for currently amended claim 13, claims 14-16 and 18 are not anticipated by

Cisco. Claim 17 has been canceled. Claim 22 depends directly from claim 19 and therefore contains each and every element of claim 19. Thus, for the reasons already set forth for currently amended claim 19, claim 22 is not anticipated by Cisco. Claims 20-21 and 23-27 have been canceled.

CONCLUSION

In view of the foregoing, it is respectfully submitted that all present claims are patentably distinct and in condition for allowance. Applicant respectfully requests that a timely Notice of Allowance be issued in this case. If the Examiner believes there are any further matters, which need to be discussed in order to expedite the prosecution of the present application, the Examiner is invited to contact the undersigned. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00004.

Respectfully submitted,

Date: August 14, 2007

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009